

# Überlegungen bei der Verwendung von AWS- Produkten in GxP-Systemen

*Januar 2016*



© 2016, Amazon Web Services, Inc. oder Tochterfirmen. Alle Rechte vorbehalten.

## Hinweise

Dieses Dokument wird nur zu Informationszwecken zur Verfügung gestellt. Es stellt das aktuelle Produktangebot und die Praktiken von AWS zum Erstellungsdatum dieses Dokuments dar. Änderungen vorbehalten. Kunden sind für ihre eigene unabhängige Einschätzung der Informationen in diesem Dokument und jedweder Nutzung der AWS-Services verantwortlich. Jeder Service wird ohne Gewähr und ohne Garantie jeglicher Art, weder ausdrücklich noch impliziert, bereitgestellt. Dieses Dokument gibt keine Garantien, Gewährleistungen, vertraglichen Verpflichtungen, Bedingungen oder Zusicherungen von AWS, seinen Partnern, Zulieferern oder Lizenzgebern. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument gehört, weder ganz noch teilweise, zu den Vereinbarungen von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

## Inhaltsverzeichnis

1	ÜBERSICHT.....	4
2	EINFÜHRUNG.....	5
2.1.1	Über AWS.....	5
2.1.2	AWS-Kunden.....	6
2.1.3	AWS-Technologie.....	7
2.1.4	AWS-Produkte.....	8
3	VERWENDUNG VON AWS-PRODUKTEN IN GXP-SYSTEMEN.....	10
3.1	Qualitätssysteme.....	10
3.1.1	Verantwortung der Geschäftsleitung.....	10
3.1.2	Personal.....	11
3.1.3	Prüfungen.....	11
3.1.4	Einkaufskontrollen.....	12
3.1.5	Produktbewertung.....	14
3.1.6	Lieferantenbewertung.....	15
3.1.7	Lieferantenvertrag.....	17
3.1.8	Aufzeichnungen und Protokolle.....	18
3.2	Lebenszyklus der Systementwicklung.....	19
3.2.1	Entwickeln.....	20
3.2.2	Validieren.....	22
3.2.3	Betreiben.....	24
3.3	Regulatorische Angelegenheiten.....	27
3.3.1	Einreichungen.....	28
3.3.2	Prüfungen.....	28
3.3.3	Datenschutzkontrollen für die personenbezogenen Daten von Forschungsteilnehmern.....	29
4	SCHLUSSFOLGERUNG.....	30
5	AM DOKUMENT Vorgenommene Änderungen.....	30
6	ANHÄNGE.....	31
6.1	Datenschutz-Ressourcen.....	31
6.2	21 CFR Part 11 kommentiert.....	32
6.3	Gemeinsame Verantwortlichkeiten in AWS-Vereinbarungen.....	34

# 1 ÜBERSICHT

Im Jahr 2006 begann Amazon Web Services (AWS), den Kunden IT-Infrastrukturprodukte in Form von Web-Services anzubieten, die jetzt allgemein als Cloud Computing bekannt sind. Heute bietet AWS eine sehr zuverlässige, skalierbare und kostengünstige Infrastruktur-Plattform an, die Hunderttausende von Unternehmen in 190 Ländern auf der ganzen Welt versorgt. Einige der wichtigsten Vorteile von Cloud Computing bestehen darin, dass Vorab-Investitionen in die Infrastruktur durch geringere variable Kosten ersetzt werden können, die je nach Nutzung skalierbar sind und es den Kunden erlauben, mehr Zeit für ihre Kernaktivitäten und weniger Zeit für undifferenzierte IT-Aufgaben aufzuwenden.

Dank der Cloud müssen Organisationen nicht mehr Wochen oder Monate im Voraus physische Geräte und IT-Infrastrukturen planen und bereitstellen. Stattdessen können sie mit automatisierten Bereitstellungstools und -methoden sofort Hunderte oder Tausende virtueller Maschinen einrichten, die Ergebnisse schneller liefern und gleichzeitig eine höhere Konsistenz der Kontrollen und weniger manuelle Fehler sicherstellen. Um von der Einführung von AWS-Produkten profitieren zu können, müssen Organisationen und deren Auditoren, die auf die Einhaltung guter klinischer, Labor- oder Fertigungspraktiken (GxP) achten müssen, neue Fähigkeiten erwerben und Änderungen an GxP-Richtlinien und -Verfahren in Betracht ziehen, die darauf ausgerichtet sind, die IT-Compliance mehr zu automatisieren und sie agiler und sicherheitsorientierter zu machen.

Dieses Whitepaper gibt eine Anleitung zur Verwendung von AWS-Produkten in Bezug auf GxP. Der Inhalt wurde in Verbindung mit AWS-Kunden aus den Bereichen Pharmazie und medizinische Geräte sowie mit Software-Partnern entwickelt, die zurzeit AWS-Produkte in ihren validierten GxP-Systemen nutzen. Um die Zweckmäßigkeit des Inhalts sicherzustellen, hat AWS darüber hinaus die Firma Lachman Consultant Services Inc. (Lachman Consultants) beauftragt, den Ansatz zu überprüfen und zu verbessern, der in diesem Whitepaper dargestellt ist. Lachman Consultants ist eine der namhaftesten Beratungsfirmen für die Einhaltung von FDA- und internationalen regulatorischen Vorschriften, die die Pharmazie- und Medizingerätebranche heute betreffen. Lachman Consultants verfügt über umfangreiche Erfahrung in der Zusammenarbeit mit Firmen im Hinblick auf die Einrichtung und Entwicklung von GxP-Systemen, einschließlich GxP-Richtlinien zur Speicherung regulierter Daten in einer Cloud-Umgebung. Weitere Informationen über Lachman Consultants finden Sie auf [www.lachmanconsultants.com](http://www.lachmanconsultants.com).

AWS-Kunden sind dennoch verpflichtet, sich mit ihren eigenen Beratern abzusprechen, um sicherzustellen, dass ihre GxP-Richtlinien und -Verfahren für die aktuelle IT, Software und die Sicherheitspraktiken geeignet sind, die AWS-Produkte verwenden.

## 2 EINFÜHRUNG

Amazon Web Services (AWS) bietet Cloud-Infrastruktur-Softwareprodukte an, die zunehmend zum Speichern und Verarbeiten vertraulicher und regulierter Daten in fast jeder Branche auf der Welt verwendet werden. Organisationen, die in den Bereichen Gesundheitswesen und Life Sciences tätig sind, profitieren von den Vorteilen der AWS Cloud und nutzen AWS-Produkte als Bestandteil ihrer regulierten IT-Systeme. Dazu gehören auch Computersysteme, die gute klinische, Labor- und Fertigungspraktiken („GxP“) für medizinische Geräte, pharmazeutische und biologische Produkte sowie andere Lebensmittel- und Medizinproduktbranchen unterstützen.

Dieses Dokument bietet Informationen für Kunden, die AWS-Produkte dazu nutzen wollen, Computersysteme aufzubauen, die elektronische Aufzeichnungen speichern oder verarbeiten, die die allgemeinen GxP-Bestimmungen und Vorgaben zur Datenintegrität einhalten müssen.

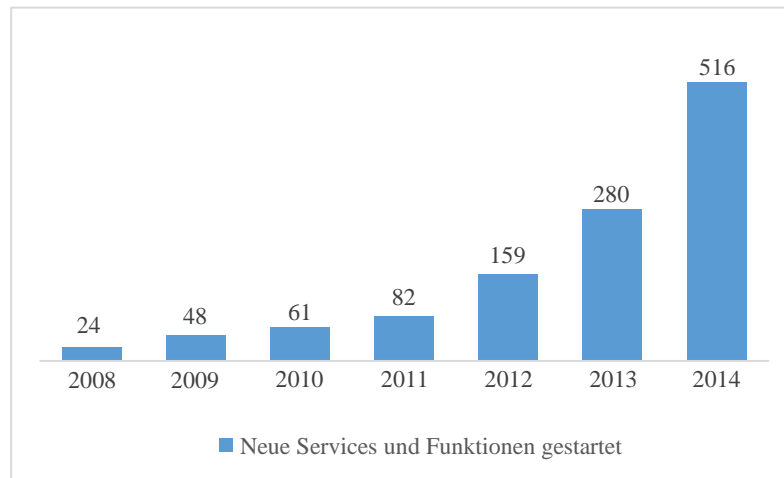
Das Dokument enthält Informationen zu folgenden Themen:

- Umfang und technologische Grundlage von AWS-Produkten,
- Überlegungen zum Qualitätssystem, die die Kunden bei der Nutzung der kommerziellen Cloud-Produkte von AWS berücksichtigen,
- Überlegungen zum Lebenszyklus der Systementwicklung für Kunden, die GxP-Systeme entwickeln, validieren und betreiben, die AWS-Produkte als Bestandteil enthalten, sowie
- Überlegungen zu regulatorischen Angelegenheiten für Kunden, die ihre systembezogenen Daten gegenüber Regulierungsbehörden offenlegen müssen.

Whitepapers mit näheren Informationen zu AWS-Produkten, Privatsphäre und Datenschutz finden Sie unter <https://aws.amazon.com/compliance/>.

### 2.1.1 Über AWS

Amazon Web Services wurde 2006 von Amazon.com (NYSE: AMZN) gegründet und ist ein etablierter Anbieter von Cloud-Services. Das Angebot umfasst Infrastruktur-Produkte auf Abonnementbasis, die auf Anfrage über das Internet von Rechenzentrum-Standorten in den USA, Australien, Brasilien, China, Deutschland, Irland, Japan, Korea und Singapur geliefert werden. Seit seiner Gründung entwickelt AWS innovative Ideen, die das Cloud Computing definieren. Dabei werden neue Produkte schnellstmöglich für die Kunden bereitgestellt und basierend auf Kunden-Feedback weiterentwickelt und verbessert. Die Innovationsgeschwindigkeit und ständige Service-Verbesserungen sind wichtige Gründe, warum sich immer mehr Organisationen bei ihren geschäftskritischen Systemen für AWS-Produkte entscheiden.



Kundenzufriedenheit und Kundenvertrauen sind grundlegende Führungsprinzipien der Teamkultur von Amazon. Während das Besitzrecht an und die Kontrolle über die Daten und Systeme beim Einsatz von AWS-Produkten bei den Kunden verbleiben, bietet AWS seinen Kunden größtmögliche Sicherheit und Transparenz, indem aktuell geltende Richtlinien zu Privatsphäre und Datenschutz eingehalten werden. Weitere Informationen finden Sie im Anhang zum Datenschutz (Seite 31).

- AMZN Corp. Info: <http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-irhome>
- Führungsprinzipien: <http://www.amazon.jobs/principles>
- Analystenberichte: <https://aws.amazon.com/resources/analyst-reports/>

### 2.1.2 AWS-Kunden

AWS hat in über 190 Ländern mehr als 1 Million aktive Kunden, die im Wesentlichen alle Branchen und Organisationstypen repräsentieren, von inhabergeführten Startups und Kleinunternehmen bis hin zu weltweiten Konzernen und Regierungsbehörden. Innerhalb der Organisationen unserer Kunden sind die primären Nutzer von AWS-Produkten die Software-Entwickler, Netzwerktechniker und Systemadministratoren, die die IT-Infrastruktur und Anwendungen der Organisation aufbauen und instand halten. AWS verfügt über eine umfangreiche Liste von Kunden-Erfolgsgeschichten, aus denen die Bandbreite an Branchen und Märkten hervorgeht, die von unseren Cloud-Produkten profitieren: <https://aws.amazon.com/solutions/case-studies/all/>.

Unter den Organisationen, die AWS-Produkte in ihren Computersystemen nutzen, sind auch solche aus den Bereichen Gesundheitswesen und and Life Sciences. Einige ihrer Erfolgsgeschichten finden Sie auf der AWS-Website zum Gesundheitswesen unter <https://aws.amazon.com/health/>.

### 2.1.3 AWS-Technologie

Amazon Web Services (AWS) ist nach einer Kerntechnologie benannt, die in alle AWS-Produkte integriert ist: Web-Services. Ein Web-Service ist ein eigenständiges, wiederverwendbares Software-Modul, das für andere Software-Module Funktionalität über Internet-Protokolle bereitstellt. Hierzu werden standardisierte Messaging-Formate wie XML<sup>1</sup> und JSON<sup>2</sup> verwendet. AWS-Produkte, auf die online über die Self-Service Management Console unter <https://aws.amazon.com/account/> zugegriffen werden kann, basieren auf zwei Arten von Web-Services, die jeweils über mehrere Schnittstellenarten verfügen:

#### Arten von Web-Services:

- Simple Object Access Protocol (SOAP)
- Representational State Transfer (REST)

#### AWS-Produktschnittstellen:

- Anwendungsprogrammierschnittstelle (API)
- Befehlszeilenschnittstelle (CLI)
- Benutzeroberfläche (GUI)

Web-Services sind nicht an bestimmte Betriebssysteme oder Programmiersprachen gebunden. Daher können Anwendungen, die in unterschiedlichen Programmiersprachen geschrieben sind und auf unterschiedlichen Plattformen laufen, nahtlos Daten über das Internet (oder Intranet) austauschen. Dies erfolgt über vordefinierte Aktionen, die von jeder Web-Service-Schnittstelle unterstützt werden. Ein großer Vorteil der Web-Service-Methode, die manchmal auch als weberorientierte Architektur bezeichnet wird, besteht darin, dass Software-Anwendungen, die Web-Services nutzen, keine Informationen darüber benötigen, wie der Web-Service aufgebaut ist oder wie die zugrunde liegenden Daten gespeichert sind. Es muss nur festgelegt werden, auf welche Aktionen die Web-Service-Schnittstelle reagieren soll. Wenn die Aktionen in der Schnittstelle verfügbar sind, haben Änderungen an den zugrunde liegenden Komponenten eines Web-Services oder das Hinzufügen von neuen Aktionen keinen Einfluss auf das Verhalten oder die Zuverlässigkeit der Anwendung. Die Liste der Web-Service-Aktionen, die von AWS-Produkten unterstützt werden, ist vollständig dokumentiert und kann online unter <https://aws.amazon.com/documentation/> abgerufen werden.

Außer der Web-Service-Technologie sind softwaredefinierte Infrastruktur-Technologien wie Virtualisierung und softwaredefinierte Netzwerke (SDN) weitere wichtige AWS-Produkte. Infrastrukturkomponenten, die früher nur als physische Spezialausrüstung verfügbar waren, beispielsweise Load Balancer und Firewalls für Netzwerke, sind jetzt auf Abruf als softwaredefinierte Ressourcen erhältlich. Dadurch verringern sich Zeit und Kosten für die Systementwicklung, während gleichzeitig durch Software-Automatisierung ein höherer Grad an Infrastruktur-Standardisierung und -kontrolle erreicht werden kann.

Der Ausbau der Software mit traditionell physischen Infrastruktur-Komponenten bewirkt in Verbindung mit den Vorteilen der weberorientierten Architektur und modernen Programmiermethoden in jeder Branche eine globale Verschiebung bei den IT-SDLCs<sup>3</sup>, den Mitarbeiterfähigkeiten und der IT-Compliance. Die Organisationen, die bereit sind, AWS-Produkte in ihren GxP-Systemen bestmöglich zu nutzen, können diese Verschiebung erkennen und sich an sie anpassen.

---

<sup>1</sup> eXtensible Markup Language

<sup>2</sup> JavaScript Object Notation

<sup>3</sup> Lebenszyklus der Systementwicklung

Vorteile von AWS-Technologie:

- **Plattformunabhängigkeit und Kompatibilität:** AWS-Produkte unterstützen Anwendungen, die in vielen verschiedenen Programmiersprachen geschrieben sind. Die Anwendungen sind nicht an bestimmte Betriebssysteme oder Hardware-Komponenten gebunden.
- **Skalierbarkeit:** Durch die Kombination aus der softwaredefinierten Infrastruktur von AWS-Produkten und modernen Programmiermethoden können AWS-Kunden ihre eigenen Computersysteme entwickeln und die Ressourcen (und damit die Kosten) schnell entsprechend den tatsächlichen Systemanforderungen hoch- oder herunterskalieren.
- **Fehlertoleranz:** AWS-Produkte unterstützen die lose Verkoppelung zwischen AWS-Produkten und Software-Anwendungen. Dadurch können die Kunden ihre GxP-Systeme so aufbauen, dass der Betrieb auch dann sichergestellt ist, wenn eine Systemkomponente oder ein AWS-Produkt zeitweilig nicht verfügbar ist.
- **Aufgabentrennung:** Die Trennung der physischen Infrastruktur-Aufgaben von der virtuellen Infrastruktur und den Software-Aufgaben des Kunden gewährleistet eine kritische Datenintegritätskontrolle, indem sichergestellt wird, dass Personen, die physischen Zugriff auf das System haben, vollständig von denen isoliert sind, die logischen Zugriff auf GxP-Daten haben.
- **Auditierbarkeit:** Die nachrichtenbasierte Kompatibilität der Web-Services ermöglicht eine einheitliche Protokollierung, Überwachung und Auditierung der Kundenkonfiguration und der Verwendung von AWS-Produkten.
- **Fokus auf Kernkompetenzen:** Der wesentliche Vorteil von AWS-Produkten besteht darin, dass unsere Kunden weniger Zeit mit undifferenzierten Aufgaben verbringen müssen und mehr Zeit haben, sich auf ihre Kernkompetenzen zu konzentrieren, die Wert für ihre Organisation schöpfen.

#### 2.1.4 AWS-Produkte

AWS entwickelt kommerzielle Cloud-Infrastruktur-Softwareprodukte und Office-Produktivitätsanwendungen. Diese Produkte sind benutzerkonfigurierbar, für allgemeine Zwecke ausgelegt und erfüllen kommerzielle IT-Standards, z. B. ISO, NIST und SOC. Damit ähneln sie anderen für allgemeine Zwecke ausgelegten IT-Produkten und -Services, beispielsweise Datenbank-Engines, Betriebssystemen, Programmiersprachen, Internetdiensteanbietern usw. Viele Organisationen stufen AWS-Produkte als kommerzielle, seriengefertigte (COTS, commercial-off-the-shelf) Infrastruktur-Softwareprodukte ein, was mit dem Gebrauch der US-Bundesregierung von AWS-Produkten als COTS-Artikel übereinstimmt, wie sie durch ein Beschaffungsprogramm auf Bundesebene mit der Bezeichnung FedRAMP definiert ist. Nach dem FedRAMP (Federal Risk and Authorization Management Program), das die Definitionen aus der US Federal Acquisition Regulation (FAR) übernimmt, sind COTS-Artikel 1) Produkte oder Dienstleistungen, die basierend auf einem aufgestellten Katalog wettbewerbsmäßig in großen Mengen auf dem kommerziellen Markt angeboten und verkauft werden, 2) ohne Modifikation oder Anpassung und 3) zu standardmäßigen Allgemeinen Geschäftsbedingungen angeboten werden. AWS-Kunden mit GxP-Anforderungen sind dafür verantwortlich, AWS-Produkte nach ihren geltenden Branchenbezeichnungen einzustufen, beispielsweise nach den Richtlinien für Computersysteme in regulierten GxP-Umgebungen als Kategorie 1 unter Good Automated Manufacturing Practices (GAMP – Bewährte automatisierte Fertigungspraktiken) und Pharmaceutical Inspection Co-operation Scheme (PIC/S – Pharmazeutischer Prüfungs-Zusammenarbeitsplan) oder – nach den Qualitätsrichtlinien für medizinische Geräte – als Software of Unknown Provenance (SOUP– Software unbekannter Herkunft), „Black Box“ OTS-Komponenten oder Datenverarbeitungsressourcen für allgemeine Zwecke.



AWS bietet über 50 Produkte in mehreren Kategorien an:

Gruppe	AWS-Produkte
<b>Datenverarbeitung</b>	Amazon EC2, Amazon EC2 Container Service, AWS Elastic Beanstalk, AWS Lambda, Auto Scaling
<b>Speicherung</b>	Amazon S3, Amazon CloudFront, Amazon EBS, Amazon EFS, Amazon Glacier, AWS Storage Gateway, AWS Snowball
<b>Datenbank</b>	Amazon RDS, Amazon DynamoDB, Amazon ElastiCache, Amazon Redshift
<b>Netzwerk</b>	Amazon VPC, AWS Direct Connect, Elastic Load Balancing, Amazon Route 53
<b>Entwickler-Tools</b>	AWS CodeCommit, AWS CodePipeline, AWS CodeDeploy, AWS Tools & SDKs
<b>Verwaltungs-Tools</b>	Amazon CloudWatch, AWS CloudFormation, AWS CloudTrail, AWS Config, AWS Management Console, AWS OpsWorks, AWS Service Catalog, Trusted Advisor, AWS Tools for Windows PowerShell
<b>Sicherheit und Identität</b>	Identity & Access Management, AWS Directory Service, Amazon Inspector, AWS CloudHSM, AWS KMS, AWS WAF
<b>Analysen</b>	Amazon EMR, AWS Data Pipeline, Amazon Elasticsearch Service, Amazon Kinesis, Amazon Kinesis Firehose, Amazon Machine Learning, Amazon QuickSight
<b>Mobile und Internet of Things (IOT)</b>	AWS IoT, AWS Mobile Hub, Amazon API Gateway, Amazon Cognito, AWS Device Farm, Amazon Mobile Analytics, AWS Mobile SDKs, Amazon SNS
<b>Anwendungs-Services</b>	Amazon API Gateway, Amazon AppStream, Amazon CloudSearch, Amazon Elastic Transcoder, Amazon FPS, Amazon SES, Amazon, SNS, Amazon SQS, Amazon SWF
<b>Produktivitätsanwendungen für Unternehmen</b>	Amazon WorkSpaces, Amazon WAM, Amazon WorkDocs, Amazon WorkMail

Details und Spezifikationen für AWS-Produkte, die globale Infrastruktur und Kundenregistrierung sind online verfügbar:

- <https://aws.amazon.com/account/>
- <https://aws.amazon.com/products/>
- <https://aws.amazon.com/documentation/>
- <https://aws.amazon.com/about-aws/global-infrastructure/>

## 3 VERWENDUNG VON AWS-PRODUKTEN IN GXP-SYSTEMEN

Obwohl AWS-Produkte als virtuelle Online-Produkte und nicht als physische, vor Ort installierte Hardware-Produkte vertrieben werden, sind die Verantwortlichkeiten für die Nutzung als Komponenten in GxP-Systemen ähnlich. Nach diesem gut eingeführten Modell haben Kunden, die kommerzielle Infrastrukturprodukte als Komponenten in ihren GxP-Systemen nutzen, Verpflichtungen in mehreren wichtigen Bereichen:

- Qualitätssysteme,
- Lebenszyklus der Systementwicklung und
- regulatorische Angelegenheiten.

### 3.1 Qualitätssysteme

Organisationen, die AWS-Produkte in GxP-Systemen nutzen möchten, sollten die Dokumentation ihres Qualitätssystems überarbeiten und aktualisieren. In diesem Abschnitt finden Sie Anleitungen zu einigen wichtigen Bereichen, die berücksichtigt werden müssen.

#### 3.1.1 Verantwortung der Geschäftsleitung

Vor der Nutzung von AWS-Produkten in Produktions-GxP-Systemen sollte geklärt werden, wie die Erstellung und Instandhaltung der AWS-Konten erfolgen soll. Da die AWS-Kontenerstellung eigenständig erfolgt und dem Kontoinhaber Anmeldeinformationen für das Stammkonto mit vollständiger Kontrolle über die Konfiguration für und den Zugriff auf das AWS-Produkt gewährt werden, sollte die Geschäftsleitung des Kunden für das AWS-Konto Richtlinien festlegen und kommunizieren, um sicherzustellen, dass alle in GxP-Systemen verwendeten Konten nachverfolgt und die Anmeldeinformationen für das Stammkonto von qualifizierten Mitarbeitern kontrolliert werden, die von der Organisation autorisiert sind. Darüber hinaus sollte für das AWS-Konto eine Passwortrichtlinie eingerichtet werden, nach der alle Kontonutzer ihr Passwort in regelmäßigen Abständen ändern müssen.

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- AWS-Kontoführungsrichtlinie
- Memo an alle Mitarbeiter mit Einkaufsberechtigung für die Organisation
- AWS-Kontoerstellungsverfahren
- Passwortrichtlinie für AWS-Kontonutzer

### 3.1.2 Personal

AWS-Kunden müssen sicherstellen, dass ihre Mitarbeiter die entsprechende Ausbildung, Schulung und Erfahrung haben, um die ihnen zugewiesenen Job-Funktionen auszuführen. Wenn zu den Job-Funktionen auch die Nutzung von AWS-Produkten in GxP-Systemen gehört, sollte die Erfahrung im Umgang mit AWS-Produkten bei der Einstellung und/oder Schulung von Mitarbeitern berücksichtigt werden. Die System-Zugriffsebene und die ausgeübten Job-Funktionen sind für die Bestimmung der erforderlichen Erfahrung relevant, und es gibt eine ganze Reihe von Job-Funktionen, die davon betroffen sein können:

- Software Engineers
- Software-Tester
- Netzwerktechniker
- Systemadministratoren
- Sicherheitstechniker
- Validierungsingenieure
- Einkaufspersonal
- Qualitätssicherungspersonal
- Auditoren
- Hinweis: Endbenutzer von GxP-Anwendungen interagieren im Allgemeinen nicht direkt mit AWS-Produkten und benötigen wahrscheinlich keine AWS-spezifische Schulung.

Die Schulung kann in Form von Sensibilisierung, Schulung *an sich* oder testbasierter Mitarbeiterqualifizierung erfolgen. AWS und das Amazon-Partnernetzwerk (APN) bieten eine ganze Reihe von Einsteiger- und laufenden Schulungen sowie Zertifizierungen für AWS-Produkte an, beispielsweise:

- Online-Dokumentation: <https://aws.amazon.com/documentation/>
- Lehrvideos: [https://aws.amazon.com/training/intro\\_series/](https://aws.amazon.com/training/intro_series/)
- Übungen im Selbststudium: <https://aws.amazon.com/training/self-paced-labs/>
- Veranstaltungen und Webinare: <https://aws.amazon.com/about-aws/events/>
- Kurse und Workshops: <https://aws.amazon.com/training/course-descriptions/>
- Partnerschulung: <https://aws.amazon.com/partners/training/>
- Berufliche Zertifizierungen: <https://aws.amazon.com/certification/>

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- Schulungspläne und -verfahren
- Arbeitsplatzbeschreibungen
- Stellenbewerbungen und Lebensläufe
- Schulungsaufzeichnungen
- Zertifizierungen mit AWS-Produkten

### 3.1.3 Prüfungen

Für Kunden, die ihre Nutzung von AWS-Produkten in GxP-Systemen überprüfen, ist es wichtig, die ständige Wirksamkeit der Systemsicherheit und Datenintegritätskontrollen sowie der System-/Software-Entwicklung (SDLC) zu bewerten. Um effektive Prüfungen der Nutzung von AWS-Produkten durchführen zu können, sollten sich IT-Auditoren mit der Web-Service-Technologie, AWS-Produkten und dem Lesen von einfachen Scripts vertraut machen, beispielsweise JSON. Idealerweise haben die Auditoren über Read-only-Zugriffsrichtlinien direkten Zugang zu den entsprechenden AWS-Kontoressourcen. Innerhalb des AWS-Kontos sollten Auditoren und Assessoren die relevanten Produktfunktionskonfigurationen und Protokolldaten überprüfen, beispielsweise:

- AWS-Konto-Anmeldeinformationen
- Organisationskontakte
- IAM-Nutzer, -Gruppen und -Rollen
- IAM-Anbieter für SAML und OpenID Connect
- Amazon EC2-Sicherheitskonfigurationen
- Ressourcenbasierte Richtlinien in anderen Services, z. B. S3
- AWS Config-Regeln
- Systemaktivitätsprotokolle in CloudTrail
- Änderungsverlauf in AWS Config
- System-Supportverläufe

AWS bietet eine Reihe von Prüfungs-Tools und Lehrressourcen zur Unterstützung von Auditoren, die die Nutzung von AWS-Produkten in GxP-Systemen überprüfen wollen:

- Whitepaper zu AWS-Prüfungen: [https://do.awsstatic.com/whitepapers/compliance/AWS\\_Auditing\\_Security\\_Checklist.pdf](https://do.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf)
- Whitepaper zu AWS-Betriebschecklisten: [https://s3.amazonaws.com/awsmedia/AWS\\_Operational\\_Checklists.pdf](https://s3.amazonaws.com/awsmedia/AWS_Operational_Checklists.pdf)
- Richtlinien zur AWS-Sicherheitsprüfung: <https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html>
- AWS CloudTrail-Produktseite: <https://aws.amazon.com/cloudtrail/>
- AWS Config-Produktseite: <https://aws.amazon.com/config/>
- AWS Trusted Advisor-Seite: <https://aws.amazon.com/premiumsupport/trustedadvisor/>
- Prüfungs-qwikLAB zum Selbststudium: <https://www.qwiklab.com/focuses/preview/1250?locale=en>
- Auditor-Schulung mit Dozent: [awsaudittraining@amazon.com](mailto:awsaudittraining@amazon.com)

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- IT-Prüfplan
- Prüfverfahren und Checklisten für AWS-Konten
- Prüfberichte für AWS-Konten
- IT-Auditorqualifikationen, Lebenslauf, Schulungsaufzeichnungen für AWS-Produkte

### 3.1.4 Einkaufskontrollen

Der traditionelle Einkauf von IT-Infrastrukturprodukten beinhaltet einen Bestellvorgang (PO) für physische Waren, die als Investitionsaufwand verbucht werden. Bei AWS-Produkten erfordert der Einkauf jedoch ein Abrechnungsverfahren nach Zählereinheiten für abonnierte Software-Produkte, die als variable Betriebsausgaben verbucht werden. Viele Life-Sciences-Organisationen haben GxP-IT-Produkteinkaufsverfahren, die für einen PO-Prozess entwickelt wurden, bei dem ein nutzungsabhängiges Produkt-Preismodell auf Abonnementbasis wie AWS nicht vorgesehen ist.

**Infrastruktur-Einkauf mit traditionellen POs**

1. IT spezifiziert Serveranforderungen
2. IT-Quellen entsprechen Server und Betriebssystem
3. IT reicht Anfrage beim Einkauf ein
4. Einkauf übermittelt PO an Lieferanten
5. Lieferant liefert Server
6. Materialabteilung erhält Lieferung
7. IT installiert Server und Betriebssystem
8. IT konfiguriert Betriebssystem
9. IT qualifiziert Server und Betriebssystem manuell,
10. Buchhaltungsabteilung bezahlt Hardware-Komponente und schreibt sie als Investitionsaufwand ab.

**Infrastruktur-Einkaufsprozess mit AWS**

1. IT spezifiziert Serveranforderungen
2. IT wählt passenden EC2 Instance-Typ aus und stellt eigenes geeignetes Betriebssystem-Abbild bereit,
3. IT startet EC2 Instance mit geeignetem Abbild und aktivierter automatischer Protokollierung,
4. IT zahlt für Nutzung von EC2 nach Zählerstand mit Betriebsaufwand-(OpEx-)Kreditkarte.

Kunden, die AWS-Produkte in GxP-Systemen nutzen, sollten ihre Einkaufsverfahren überprüfen, um sicherzustellen, dass diese ein Preismodell auf Abonnementbasis mit Online-Bereitstellung verwalten können. Bei dieser Überprüfung sollten die IT, der Einkauf und die Qualitätssicherungsteams der Organisation einbezogen werden. Die Prüfung sollte auch die Bestellung, Annahme und Zahlungen sowie die AWS-Kontenverwaltung umfassen. AWS stellt Dokumentationen bereit, um Organisationen beim Verstehen und Verwalten ihrer AWS-Kontofakturierung zu unterstützen.

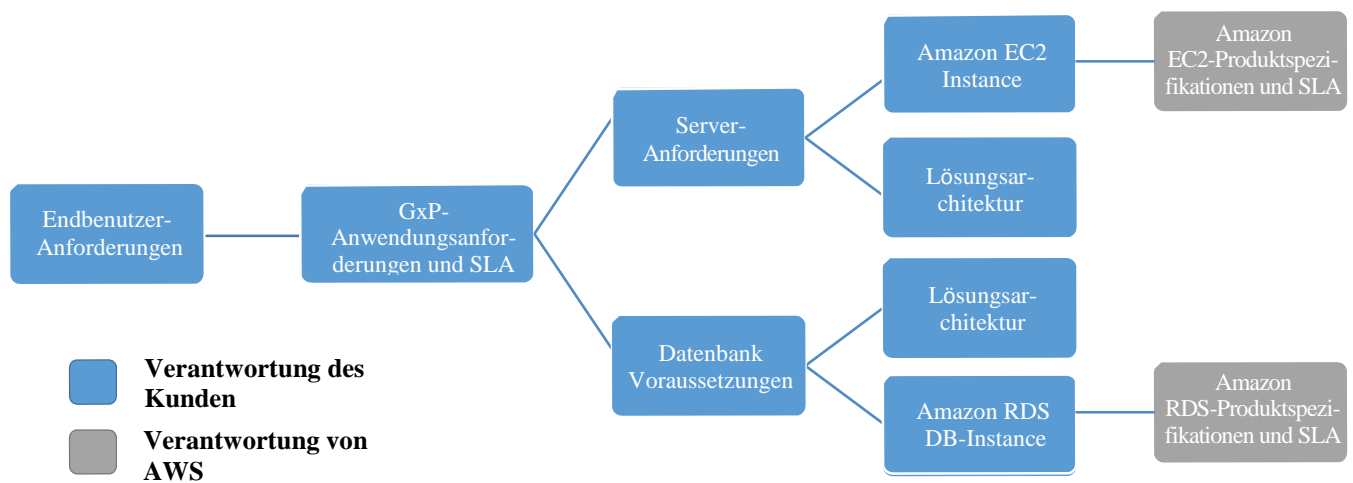
- Whitepaper zur AWS-Fakturierung und Kostenverwaltung: <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/awsaccountbilling-aboutv2.pdf>
- Überblick über Ihre Nutzung mit detaillierten Fakturierungsberichten: <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/detailed-billing-reports.html>
- AWS – einfacher Monats-Fakturierungsrechner <http://calculator.s3.amazonaws.com/index.html>
- Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten zu optimieren:

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- Einkaufsverfahren
- AWS – detaillierte Fakturierungsberichte
- PDF-Rechnung per E-Mail

### 3.1.5 Produktbewertung

Sicherzustellen, dass die eingekauften Waren und Dienstleistungen den angegebenen Anforderungen entsprechen, ist eine wesentliche Anforderung bei GxP-Kontrollen. Bei kommerziell verfügbaren Infrastrukturkomponenten wie AWS-Produkten kann recht einfach sichergestellt werden, dass die Produktspezifikationen den Benutzeranforderungen entsprechen, weil alle Schnittstellenspezifikationen und Vereinbarungen für AWS-Produkte vollständig dokumentiert und für die Kunden zur Überprüfung verfügbar sind. Da AWS keine AWS-Produkte oder SLAs für einzelne Kunden spezifisch anpasst, können die Kunden einfach ihre GxP-Anwendungsanforderungen mit den entsprechenden AWS-Produktspezifikationen und SLAs vergleichen. Wenn ein Kunde beispielsweise eine COTS-konfigurierbare Software-Anwendung mit dem Amazon EC2-Produkt und Amazon RDS-Produkt von AWS betreiben will, sollte er zuerst die Server-Anforderungen der Anwendung (CPU, Arbeitsspeicher usw.) und die Datenbankanforderungen dokumentieren und dann die Amazon EC2- und Amazon RDS-Produktseiten besuchen, um die virtuelle Serverfamilie (z. B. EC2 Instance-Typ) und den Datenbanktyp (z. B. DB Instance-Typ) zu ermitteln, die die Anwendungsanforderungen erfüllen.



Es ist wichtig anzumerken, dass die GxP-System-SLA keine direkte Funktion der jeweiligen AWS-Produkt-SLAs ist; stattdessen ist die GxP-System-SLA eine Funktion der Konfiguration und Nutzung von AWS-Produkten des Kunden (d. h., seiner Lösungsarchitektur). Wenn beispielsweise eine GxP-Anwendung einen höheren Grad an Verfügbarkeit erfordert, als dies von dem/den jeweiligen AWS-Produkt(en) bereitgestellt wird, kann der Kunde seine Lösung so aufbauen, dass der höhere Grad an Verfügbarkeit erreicht wird. Deshalb muss bei der Bewertung der Eignung von AWS-Produkten für ein bestimmtes GxP-System die Gesamt-Lösungsarchitektur berücksichtigt werden.

Beim Bewerten von AWS-Produkten für kundenspezifische Anwendungen (GAMP Kategorie 5) oder medizinische Geräte verlangt die Produkteinstufung, dass GxP-Kunden in ihrer SDLC-Planungsphase gleichermaßen den Systemkontext, potenzielle Architekturen und Konstruktionen sowie verfügbare AWS-Produkte analysieren. Um sowohl bestehende als auch potenzielle Kunden bei der Ermittlung zu unterstützen, ob bestimmte AWS-Produkte ihre Anwendungsanforderungen erfüllen, veröffentlicht AWS technische Produktdokumentation online und bietet Kunden die Möglichkeit, AWS-Produkte auszuprobieren, bevor der GxP-Systemaufbau genehmigt wird.

- AWS-Produktdokumentation: <https://aws.amazon.com/documentation/>

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- SDLC-Verfahren
- GxP-Systemanforderungen und Risikobewertung
- Lösungsarchitektur für GxP-System
- AWS-Produktbewertung

### 3.1.6 Lieferantenbewertung

Organisationen mit GxP-Anforderungen müssen potenzielle Lieferanten, Auftragnehmer und Berater aufgrund ihrer Möglichkeiten, die angegebenen Anforderungen zu erfüllen, bewerten und auswählen. Wenn ein Kunde eine Produktbewertung durchgeführt und entschieden hat, dass AWS-Produkte die Anforderungen seiner GxP-Systemarchitektur erfüllen, kann eine Lieferantenbewertung durchgeführt werden, um zu ermitteln, ob AWS die AWS-Produkte gemäß den veröffentlichten Schnittstellenspezifikationen und SLAs zuverlässig bereitstellen kann.

AWS betreibt ein branchenführendes Management-Kontrollnetzwerk, das die aktuellen Standards für Qualität, Sicherheit und Vertrauenswürdigkeit für kommerzielle IT-Organisationen erfüllt. Compliance-Bewertungen werden bei AWS-Kontrollen in regelmäßigen Abständen von qualifizierten Drittanbieter-Auditoren durchgeführt. Compliance-Berichte über diese Bewertungen werden den Kunden zur Verfügung gestellt, damit sie AWS als Lieferanten bewerten können. In den AWS-Compliance-Berichten wird der Umfang der bewerteten AWS-Produkte und der Regionen angegeben. Sie enthalten auch eine Einhaltungsbestätigung des Bewerters.

Kontrollen	Bewertungs-kriterien	Auditor	Compliance-Bericht
ISO 27001	ISO/IEC 17021 & 27006	EY CertifyPoint	<a href="https://aws.amazon.com/compliance/iso-27001-faqs/">https://aws.amazon.com/compliance/iso-27001-faqs/</a>
ISO 27017	ISO/IEC 17021 & 27006	EY CertifyPoint	<a href="https://aws.amazon.com/compliance/iso-27017-faqs/">https://aws.amazon.com/compliance/iso-27017-faqs/</a>
ISO 9001	ISO/IEC 17021	EY CertifyPoint	<a href="https://aws.amazon.com/compliance/iso-9001-faqs/">https://aws.amazon.com/compliance/iso-9001-faqs/</a>
SOC 1	AT 801 &	EY	<a href="https://aws.amazon.com/compliance/soc-faqs/">https://aws.amazon.com/compliance/soc-faqs/</a>
SOC 2			

Kontrollen	Bewertungs-kriterien	Auditor	Compliance-Bericht
SOC 3	AT 101 Controls , TSP Sec. 100 Trust & Attestation		
FedRAMP/N IST 800- 53r4	NIST 800-53a	Veris Group	<a href="https://www.fedramp.gov/marketplace/compliant-systems/amazon-web-services-aws-eastwest-us-public-cloud/">https://www.fedramp.gov/marketplace/compliant-systems/amazon-web-services-aws-eastwest-us-public-cloud/</a>
PCI-DSS v3.1 Level 1	PCI DSS Security Audit Procedure	Coalfire	<a href="https://aws.amazon.com/compliance/pci-dss-level-1-faqs/">https://aws.amazon.com/compliance/pci-dss-level-1-faqs/</a>

Es sind weitere Online-Ressourcen verfügbar, die den Kunden Einblicke in AWS-Sicherheitsprozesse sowie den aktuellen und vergangenen Leistungsverlauf von AWS-Produkten gewähren:

- AWS-Whitepaper zu Risiko und Compliance, Anhang A: CSA-Fragebogen  
[https://do.awsstatic.com/whitepapers/compliance/AWS\\_Risk\\_and\\_Compliance\\_Whitepaper.pdf](https://do.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf)
- Überblick über das AWS-Whitepaper zu den Sicherheitsprozessen  
<https://do.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>
- AWS Service Health Dashboard und Statusverlauf  
<http://status.aws.amazon.com/>

GxP-Kunden sollten ihre Lieferantenbewertungsverfahren aktualisieren, um sicherzustellen, dass AWS-Produkte in alle Lieferantenkategorien aufgenommen werden können. Bei GxP-Kunden, die bereits Erfahrung mit der Nutzung von AWS-Produkten in ihren Nicht-GxP-Systemen haben, sollte die GxP-Lieferantenbewertung von AWS auch eine Leistungsverlaubbewertung dieser Nicht-GxP-Systeme einschließlich aller systembezogenen Probleme enthalten, die AWS zugeschrieben werden konnten *und* die nicht über die Lösungsarchitektur des Kunden behoben werden konnten.

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- GxP-Lieferantenklassifizierungs- und -bewertungsverfahren
- Leistungsbewertung von Nicht-GxP-Systemen
- AWS-Lieferantenbewertungsdaten, einschließlich Lieferantenfragebogen
- AWS-Lieferantengenehmigungsbericht
- AWS-Compliance-Berichte und Whitepapers
- Siehe auch Lieferantenverträge (Seite 17)



### 3.1.7 Lieferantenvertrag

Verträge mit IT-Lieferanten sind wichtig für Organisationen mit GxP-Systemen. Dazu gehören auch dokumentierte, klare Aussagen des IT-Lieferanten zu gemeinsamen Verantwortlichkeiten und Verpflichtungen, um die Organisation über wesentliche Änderungen am Produkt des Lieferanten zu benachrichtigen. Da AWS-Produkte standardisiert und für jeden Kunden identisch sind, sind AWS-Produktverträge ebenfalls standardisiert und beinhalten Definitionen der Verpflichtungen sowohl seitens AWS als auch des Kunden sowie Benachrichtigungsmechanismen bei Änderungen an AWS-Produkten.

Die AWS-Verträge sind unten aufgelistet, und im Anhang (Seite 34) ist eine Tabelle mit GxP-relevanten Verantwortlichkeiten enthalten, die in diesen AWS-Verträgen erwähnt sind.

- Kundenvertrag <https://aws.amazon.com/agreement/>
- Unternehmensvertrag AWS-Vertrieb kontaktieren
- Sicherheitszusatz AWS-Vertrieb kontaktieren
- Kunden-Support <https://aws.amazon.com/premiumsupport/>
- Service-Bedingungen <https://aws.amazon.com/service-terms/>
- Richtlinie zu zulässiger Nutzung <https://aws.amazon.com/aup/>
- Produktspezifische Service Level Agreements (SLAs):
  - Amazon S3 <https://aws.amazon.com/s3/sla/>
  - Amazon EC2 und EBS <https://aws.amazon.com/ec2/sla/>
  - Amazon RDS <https://aws.amazon.com/rds/sla/>
  - Route53 <https://aws.amazon.com/route53/sla/>
  - CloudFront <https://aws.amazon.com/cloudfront/sla/>
- Zusatz zur Datenverarbeitung <https://aws.amazon.com/compliance/eu-data-protection/>

Kunden, die AWS-Produkte in GxP-Systemen nutzen, sollten den Grad an Support, den sie von AWS benötigen, sorgfältig abwägen. Es gibt vier Stufen von AWS Support: Basic, Developer, Business und Enterprise. Jede Stufe beinhaltet eine unterschiedliche Klassifizierung der Fallschwere und der Reaktionszeiten. Abhängig vom Support-Szenario des Kunden, beispielsweise die Fehlersuche nach einem systembezogenen Problem im Fall einer behördlichen Inspektion aus wichtigem Grund (siehe Seite 28), bestimmt die AWS-Supportstufe die Reaktionszeiten auf die Anfrage des Kunden. Viele aktuelle GxP-Kunden von AWS entscheiden sich für die Business- oder Enterprise-Supportstufe, um diese Szenarios abzudecken.

Die Kunden sollten ihre IT-Lieferantenvertragsrichtlinien überprüfen und nötigenfalls aktualisieren, um sicherzustellen, dass sie mit dem standardisierten Betriebs- und Vertragsmodell von AWS kompatibel sind. Dies ist insbesondere erforderlich bei Organisationen, die bereits zuvor Dienstleistungen von Anbietern von verwalteten Services, Nischen-GxP-Services und Co-Location-Anbietern genutzt haben, bei denen die Lieferanten ihre Dienstleistungen anpassen und im Auftrag des Kunden die Anwendungsentwicklung, Validierung und Instandhaltung durchführen.

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- IT-Lieferantenvertragsrichtlinie
- Die oben aufgeführten zutreffenden Verträge

### 3.1.8 Aufzeichnungen und Protokolle

Life-Sciences-Organisationen müssen für jedes GxP-System die aufbewahrungspflichtigen Aufzeichnungen und die als GxP-Nachweis benötigten Protokolle benennen und die Integrität und Verfügbarkeit der Aufzeichnungen über den gesamten Aufbewahrungszeitraum sicherstellen. Bei der Nutzung von AWS-Produkten in GxP-Systemen bestehen die aufbewahrungspflichtigen Aufzeichnungen hauptsächlich aus den im GxP-System gespeicherten Kundendaten, dem GxP-Systemsoftware-Code und den SDLC-Aufzeichnungen sowie den vom System generierten Protokollen und Prüfpfaden, die im AWS-Konto des Kunden verfügbar sind. Aufgrund des hohen Grades an Automatisierung, der sich mit AWS-Produkten und modernen SDLC-Methoden erreichen lässt, werden viele der aufbewahrungspflichtigen Aufzeichnungen, die früher manuell erstellt werden mussten – beispielsweise ausgedruckte Installationsprotokolle – heute durch die Ausführung von Programmbefehlen erstellt. Diese zuverlässigere Methode zum Erstellen von Aufzeichnungen verringert die Variabilität und verbessert nachweislich die Datenintegrität, sowohl in Bezug auf die GxP-Daten als auch auf die SDLC.

Da sich die mit automatisierten IT-Prozessen erstellten Aufzeichnungstypen und -formate stark von manuell erstellten Aufzeichnungen unterscheiden, sollten GxP-Kunden die Aufzeichnungstypen und -formate festlegen, die sie zur Einhaltung und Entwicklung ihrer Richtlinien zur Aufbewahrung von Aufzeichnungen benötigen. AWS-Produkte, die in medizinischen GxP-Geräten genutzt werden, sollten auch in Bezug auf ihre Auswirkung beim Erstellen von Aufzeichnungen in der Design History File (DHF) und dem Device Master Record (DMR) überprüft werden. In vielen Fällen sind Aufzeichnungen, die programmatisch von AWS-Produkten generiert werden, beispielsweise Prüfpfade und Alarme, vollständig portabel und können entweder im AWS-Konto des Kunden oder an einem alternativen Speicherort gesichert werden.

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- Aufbewahrungszeitplan für Unterlagen
- Richtlinien zu Unterlagentypen und -formaten
- Verfahren zum Aufbewahren von Aufzeichnungen
- CloudTrail-Protokolle
- CloudWatch-Alarme
- S3- und Glacier-Aufbewahrungsrichtlinien und -Lebenszyklusregeln
- AWS-Supportverläufe

### 3.2 Lebenszyklus der Systementwicklung

Außer den Qualitätssystemanforderungen für die Organisation muss jedes GxP-System bestimmte Funktionen und einen kontrollierten SDLC-Prozess für deren Bereitstellung aufweisen. Die spezifischen Funktionen und SDLC-Kontrollen, die für die einzelnen Systeme gelten, hängen von einer Vielzahl von Faktoren ab und sind aus Vorschriften wie 21 CFR Parts 11 und 820 in den USA, Annex 11 und 93/42/EEC in der EU sowie ihren internationalen Äquivalenten abgeleitet. Insgesamt sollen diese behördlichen Regelungen sicherstellen, dass das GxP-System seinen beabsichtigten Zweck erfüllt und dass die Daten vertrauenswürdig und zuverlässig sind, da sie zur Bereitstellung medizinischer Versorgung oder zum Treffen von Entscheidungen über die Sicherheit und Wirksamkeit medizinischer Produkte verwendet werden können, beispielsweise Nahrungsmittel, Medikamente und medizinische Geräte sowie für Tiernahrungsmittel und -medikamente.

#### **SDLC-Kontrollen für GxP-Systeme:**

- Kontrolle des Aufbaus und der Entwicklung, um sicherzustellen, dass die angegebenen Anforderungen erfüllt werden
- Validierung von Software-Anwendungen und Qualitäts-Infrastruktur, um Genauigkeit, Zuverlässigkeit und Erfüllung der beabsichtigten Leistung sicherzustellen
- Änderungskontrolle und Änderungsverlauf bei Systemen, die in einer Produktionsumgebung betrieben werden, einschließlich Systembenutzer-Dokumentation
- Überwachungssystem in der Produktionsumgebung, um Abweichungen zu erfassen und darauf zu reagieren (z. B. Fehler)
- Dokumentieren und Verarbeiten von systembezogenen Beschwerden und Benutzer-Supportvorgängen
- Aufbewahrung von SDLC-Aufzeichnungen und GxP-Daten über den gesamten System-Lebenszyklus, einschließlich Abschreibung

#### **In GxP-Systemen benötigte Funktionen:**

- Möglichkeit zum Erstellen genauer und vollständiger Kopien von GxP-Daten in für Menschen und Maschinen lesbarer Form
- Dateneingangsvalidierung und Datenintegritätsprüfungen
- Benutzer-Zugriffskontrollen und Autorisierungssprüfungen für Benutzeraktionen
- Sichere, computergenerierte Prüfpfade mit Zeitstempel von Benutzeraktionen und Datenänderungen
- Prüfungen zur Durchsetzung der zulässigen Sequenzierung von Schritten (z. B. Workflow-Durchsetzung)
- Verschlüsselung von Daten im Transit und im Ruhezustand
- Verzeichnisse mit elektronischen Signaturen für Benutzer mit Datenänderungsberechtigung
- Verknüpfung zwischen elektronischen Signaturen und den damit verbundenen Daten

Diese Anforderungen mit dem herkömmlichen IT-Infrastrukturmodell zu erfüllen, ist umständlich, weil die softwarebasierte Anwendungs-SDLC und die hardwarebasierte Infrastruktur-SDLC recht unterschiedlich sind und die von verschiedenen Herstellern erstellten physischen Infrastruktur-Komponenten eine Reihe manueller und Verfahrenskontrollen erfordern, um sicherzustellen, dass die Konfigurationen aufrechterhalten werden und die Änderungen über die gesamte Infrastruktur verfolgbar sind. Bei AWS-Produkten ersetzen die Unternehmen ihre physischen Infrastruktur-Produkte durch eine aufeinander abgestimmte Suite virtualisierter Infrastrukturprodukte. Dadurch ist es möglich, die gesamte Infrastruktur als Software-Code zu erstellen und zu verwalten. Die Kunden können AWS-Produkte wie Amazon EC2 nicht nur dazu nutzen, identische virtuelle Server über versionsgesteuerte Abbilder zu starten – die gesamte Infrastruktur einschließlich Speicher, Datenbank und Netzwerk kann mit softwarebasierten Konfigurationsvorlagen entwickelt, versionsgesteuert und bereitgestellt werden. Diese „Infrastruktur als Code“ ermöglicht ein ungeahntes Maß an Kontrolle, Einheitlichkeit und Automatisierung der SDLC für das gesamte System, einschließlich Anwendung und Infrastruktur. Dies bedeutet auch, dass die Synchronisierung der Umgebungen für Entwicklung, Test und Produktion erheblich weniger Aufwand erfordert als bei herkömmlichen IT-Modellen.

Obwohl AWS-Produkte im Allgemeinen mit SDLC-Methoden wie DevOps verknüpft sind, werden SDLCs wie Waterfall und V-Modell vollständig unterstützt. In diesem Abschnitt werden anhand eines verallgemeinerten dreiphasigen SDLC-Beispiels einige Überlegungen für Kunden erklärt, die AWS-Produkte in GxP-Systemen nutzen.

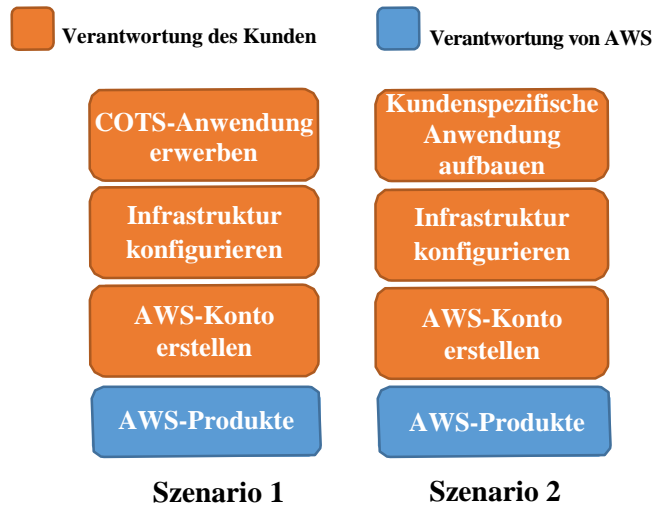


### 3.2.1 Entwickeln

GxP-Systeme müssen nach dokumentierten Verfahren entwickelt werden, durch die sichergestellt wird, dass die Systeme die angegebenen Anforderungen erfüllen. Kunden, die AWS-Produkte in GxP-Systemen verwenden, sind für alle GxP-Systementwicklungsaktivitäten vollständig verantwortlich. Dazu gehören das Planen, Codieren, Aufbauen, Konfigurieren, Testen, Validieren und Bereitstellen der Anwendungen sowie das Gestalten, Beschaffen, Konfigurieren, Orchestrieren, Bereitstellen, Qualifizieren und Betreiben der softwaredefinierten Infrastruktur. AWS konstruiert oder entwickelt keine GxP-Systeme im Kundenauftrag. Für AWS-Produkte gibt es jedoch ausführliche Benutzerdokumentationen und Whitepapers, die GxP-Systemingenieure als Beiträge für den Systemaufbau und die Entwicklungsaktivitäten verwenden können.

Die Eingangsanforderungen für den Aufbau von GxP-Systemen sollten auch Cyber-Sicherheitsanforderungen beinhalten. AWS empfiehlt, dass die Kunden einen Sicherheitsplan für das GxP-System entwickeln, der an einem anerkannten Sicherheits-Planungsstandard ausgerichtet ist, z. B. NIST Special Publication 800- 13 und alle anwendbaren behördlichen Leitfäden, beispielsweise „Content of Premarket Submissions for Management of Cybersecurity in Medical Devices“ von der FDA.

Obwohl die Kunden mit AWS-Produkten viele verschiedene Systemtypen erstellen können, gibt es zwei grundlegende Entwicklungsszenarios: 1) Erwerb einer COTS-Anwendung oder 2) Aufbau einer kundenspezifischen Anwendung.



Bei der Bewertung von COTS-Softwarepaketen für die Nutzung mit AWS-Produkten sollten GxP-Kunden die Technologiepartner des AWS-Partnernetzwerks (APN) und den AWS Marketplace in ihre Bewertung einschließen. Die AWS-Technologiepartner bieten Softwarelösungen an, die entweder auf der AWS-Plattform gehostet oder in diese integriert sind. Der AWS Marketplace ist ein Online-Shop, in dem Kunden AWS-kompatible Software direkt über ihr AWS-Konto kaufen und bereitstellen können.

- APN-Technologiepartner <https://aws.amazon.com/partners/technology/>
- AWS Marketplace <https://aws.amazon.com/marketplace/>

AWS-Produkte können auch mit handelsüblichen Software-Anwendungen von außerhalb des APN-Netzwerks oder des AWS Marketplace verwendet werden. Allerdings müssen die Kunden die Lizenzvereinbarungen der Anwendung überprüfen und eine Produktbewertung durchführen (siehe Seite 14 oben), um die Kompatibilität der Anwendung mit AWS-Produkten zu ermitteln. Auch hierbei können die APN-Beratungspartner Unterstützung geben: <https://aws.amazon.com/partners/consulting/>.

Obwohl Life-Sciences-Organisationen es im Allgemeinen vorziehen, ihre Software-Anwendungen zu kaufen, anstatt sie zu erstellen, besteht ein wesentlicher Vorteil der Kombination von AWS-Produkten mit modernen SDLC-Methoden in der Möglichkeit, kundenspezifische Software-Lösungen schnell, wiederholt und zuverlässig bereitzustellen. Viele der traditionellen Gründe, die Organisationen vom Aufbau ihrer Software abgehalten haben, beispielsweise der manuelle Aufbau von Softwarepaketen aus Quellcode oder die manuelle Durchführung von Regressionstests, haben jetzt keinen Bestand mehr, da vollständig automatisierte Tools die Verzögerungen und Fehler verringert oder eliminiert haben, die durch manuelle Entwicklungsaktivitäten verursacht wurden.

AWS-Produkte wie AWS OpsWorks, AWS CodeCommit und AWS CodePipeline stellen für die Systemingenieure flexible, konfigurierbare Tools bereit, mit denen sie die jeweiligen Anforderungen für ihre Organisation erfüllen können, wobei gleichzeitig die Implementierung von SDLC-Kontrollen für die Software-Entwicklungsaktivitäten rationalisiert wird.

Wenn ein Kunde ein GxP-System entwickelt hat und es für eine Validierung, Produktion oder andere Umgebung bereitgestellt werden kann, machen AWS-Produkte wie Amazon Machine Images (AMI), AWS CloudFormation, AWS CodeDeploy und AWS Elastic Beanstalk eine konsistente und kontrollierte Bereitstellung einfach und wiederholbar. Diese Tools bieten auch die Möglichkeit, versionsgesteuerte Kopien der gesamten Systemumgebung zu erstellen, vom Netzwerk-Stapel über die Datenbank und Speicher-Volumes bis hin zu den Datenverarbeitungs-Instances. Diese versionsgesteuerten Kopien können zur Archivierung und Änderungsverwaltung oder zur Bereitstellung von neuen Entwicklungs-/Testumgebungen zur fortlaufenden Entwicklung oder Fehlersuche aufbewahrt werden.

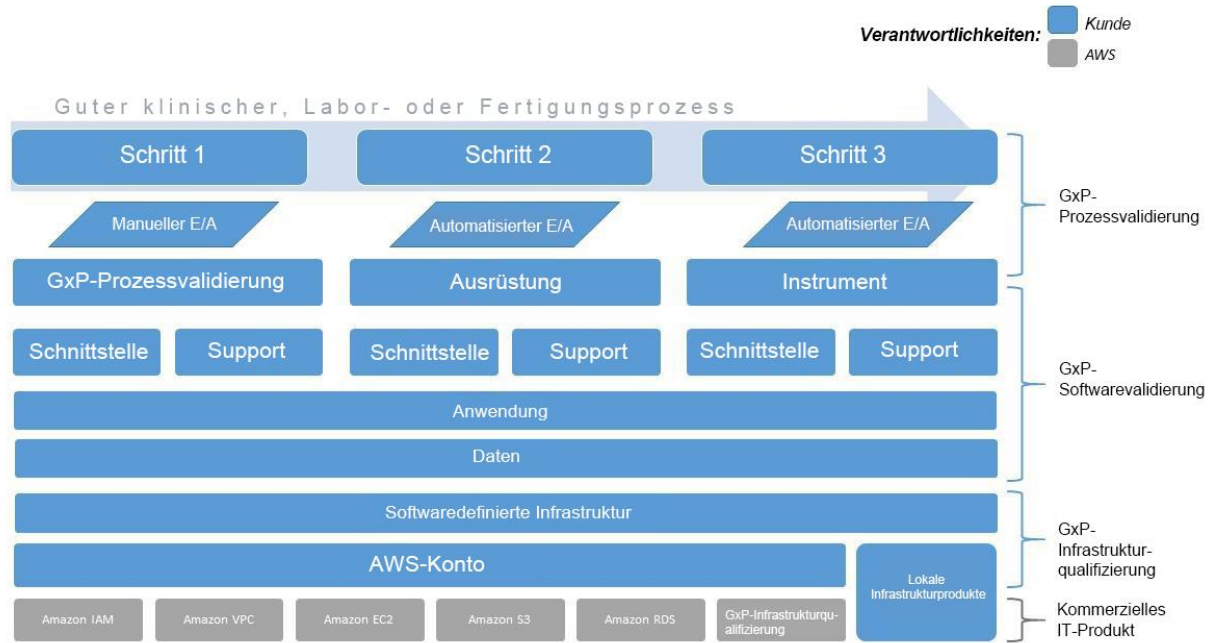
Dieses neue Modell der fortlaufenden Entwicklung und Bereitstellung ist einer der Hauptgründe, warum so viele Kunden in so vielen Branchen ihr Geschäft mit AWS-Produkten modernisieren. Um diese Vorteile in ihren GxP-Systemen nutzen zu können, müssen die Kunden möglicherweise ihre Entwicklungsmethoden und -verfahren überprüfen und aktualisieren.

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- SDLC-Verfahren
- Systemaufbau- und -entwicklungsplan
- Gefährdungsbeurteilungsverfahren
- Code-Prüfung SOP
- Anwendungsfälle und Benutzergeschichten oder andere Anforderungsspezifikation
- SLA-Kriterien für Endbenutzer, einschließlich Endbenutzer-Support
- Software-Architekturspezifikationen
- Funktionsanforderungen der Anwendung
- Vorläufige Risiko- (oder Gefahren-) Analyse für medizinische und mobile GxP-Anwendungen
- AWS CloudTrail- und Config-Protokolle
- Quellcode der Anwendung
- EC2 AMIs und CloudFormation-Vorlagen
- Code-Bereitstellung SOP

### 3.2.2 Validieren

GxP-Anwendungen müssen validiert werden, um sicherzustellen, dass die Software-Spezifikationen den Anforderungen des Benutzers entsprechen. Die Software-Infrastruktur, unter der die GxP-Anwendung läuft, muss qualifiziert werden, um sicherzustellen, dass sie die Systemanforderungen für die Anwendung erfüllt. Da AWS-Produkte vollständig auf Self-Service-Basis bereitgestellt werden, sind Kunden, die AWS-Produkte in GxP-Systemen nutzen, in vollem Umfang für die gesamte Software-Validierung und Infrastruktur-Qualifizierung innerhalb ihres AWS-Kontos verantwortlich. Da AWS keine Anwendungen im Namen von Kunden entwickelt oder verwaltet und auch keine kundenspezifische Infrastruktur bereitstellt oder konfiguriert, kann AWS keine GxP-Validierungs- oder Qualifizierungsaktivitäten im Namen von Kunden durchführen. AWS ist dafür verantwortlich sicherzustellen, dass AWS-Produkte die AWS-Produktspezifikationen, SLAs und kommerziellen IT-Standards erfüllen, und GxP-Kunden sind für die Validierung der GxP-Systeme verantwortlich, die sie mit AWS-Produkten aufbauen.



Die Installation, Instanziierung und Bereitstellung von Anwendungen und Infrastruktur sind bei AWS-Produkten völlig anders als bei herkömmlichen Medien mit physischer Infrastruktur und Installation. Bei der früher üblichen physischen Infrastruktur-Hardware waren die Installationsaktivitäten vorwiegend manuell und protokollgesteuert. Die Protokolle wurden in der Regel für jede Systemkomponente einzeln entwickelt und vorab genehmigt, dann von einem Bediener manuell ausgeführt, während ein Prüfer darauf achtete, dass jeder Schritt korrekt ausgeführt wurde. Abschließend wurde das Protokoll von einem Qualitätsbeauftragten überprüft und genehmigt. Mit der Entwicklung von IT-SDLCs und zunehmender Server-Virtualisierung verschoben sich die Validierungsaktivitäten von protokoll- zu verfahrensgesteuerten Aktivitäten, obwohl diese immer noch überwiegend manuell erfolgten. Einige Organisationen erstellten mithilfe eines Protokolls ein qualifiziertes „Gold-Abbild“ und verwendeten dieses Abbild anschließend zum Erstellen eines virtuellen Servers nach einem bestimmten Verfahren.



Im Cloud-Zeitalter, in dem die Infrastruktur über Software definiert wird, haben GxP-Systemingenieure die Möglichkeit, den gesamten Systemstapel über die Version zu steuern und die Bereitstellung mit versionsgesteuerten Infrastrukturvorlagen zu automatisieren. Bei AWS-Kunden besteht eine der gängigen Praktiken darin, qualifizierte Systemvorlagen zu erstellen und diese in Verbindung mit automatisierten Bereitstellungs-Tools zur Bereitstellung einzelner Ressourcen sowie gesamter Entwicklungs-, Test- und Validierungsumgebungen zu verwenden. Die Webservice-API-Technologie, die in jedes AWS-Produkt integriert ist, erlaubt es auch, API-Verifizierungstools von Drittanbietern, z. B. RunScope und SoapUI, viel häufiger zum Qualifizieren und Validieren von erwartetem Systemverhalten zu nutzen als dies früher mit der manuellen, periodischen Validierung möglich war.

Wegen dieses Paradigmenwechsels von zeitpunktbezogenen manuellen Aktivitäten zu kontinuierlichen automatischen Aktivitäten sollten die GxP-Änderungskontroll- und Validierungspraktiken, die viele Life-Sciences-Organisationen bei ihren herkömmlichen Hardware-Infrastrukturen anwenden, überprüft und aktualisiert werden, damit sie dem automatisierten Infrastrukturmodell gerecht werden, das bei der Nutzung der kommerziellen Cloud-Produkte von AWS als Komponenten von GxP-Systemen zur Anwendung kommt.

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- SDLC-Verfahren
- Validierungsverfahren
- IT-Qualifizierungsverfahren
- Automatisiertes Bereitstellungsverfahren
- AWS CloudTrail- und Config-Protokolle
- Quellcode der Anwendung
- EC2 AMIs und CloudFormation-Vorlagen

### 3.2.3 Betreiben

Das Entwickeln, Ausführen, Kontrollieren und Überwachen von GxP-Systemen bei Produktionsvorgängen ist wichtig, um sicherzustellen, dass sie auch weiterhin die Spezifikationen erfüllen. Wenn Endbenutzerprobleme oder Systemabweichungen auftreten, müssen Organisationen mit GxP-Systemen auch ein Verfahren zum Behandeln, Korrigieren und Verhindern solcher Probleme unterhalten. AWS-Produkte können für diese Aktivitäten genutzt werden. AWS führt jedoch keine GxP-Systemoperationen und Überwachungsaktivitäten von GxP-Systemen im Namen von Kunden durch.



GxP-Systemprinzip	Zusammenfassung der Anforderungen	Überlegungen
<b>Änderungskontrolle</b>	Änderungen an GxP-Systemen in der Produktion sollten verifiziert oder validiert werden, um sicherzustellen, dass das System die zuvor festgelegten Benutzeranforderungen erfüllt.	<p>Kunde: Der Kunde definiert die Systembenutzer-Anforderungen. Er konfiguriert und qualifiziert AWS-Produkte so, dass sie diese Anforderungen erfüllen. Die Kunden sind dafür verantwortlich, die Änderungen, die sie an den Benutzeranforderungen und Produktkonfigurationen vornehmen, zu verifizieren und zu validieren.</p> <p>AWS: AWS hat keine Kontrolle über die Kundenanforderungen oder Produktkonfigurationen. Demzufolge kann AWS keine GxP-Systemänderungen im Namen von Kunden verifizieren oder validieren. AWS verifiziert keine Änderungen an AWS-Produkten, um sicherzustellen, dass Produktspezifikationen und SLAs eingehalten werden.</p>
<b>Service Level Agreement</b>	Es müssen formelle Vereinbarungen zwischen GxP-Systemanwendern und Dritten geschlossen werden, einschließlich IT-Abteilungen, die das GxP-System instand halten.	<p>Kunde: Der Kunde definiert das Service Level Agreement für das GXP-System. Er muss AWS-Produkte konfigurieren und verwenden, um das SLA zu erfüllen.</p> <p>AWS: AWS-Produkt-SLAs unterscheiden sich von GxP-System-SLAs. AWS hat keine Kontrolle über oder Einblick in die SLAs, die der Kunde für das System erstellt.</p> <p>Siehe Anhang 4.3, Gemeinsame Verantwortlichkeiten in AWS-Vereinbarungen</p>
<b>Endbenutzer-Support</b>	GxP-Systeminhaber sollten Verfahren einrichten, um Support für die Endbenutzer bereitzustellen.	<p>Kunde: Die Kunden sind dafür verantwortlich, Support für die Endbenutzer des GxP-Systems bereitzustellen.</p> <p>AWS: AWS stellt keinerlei Support oder Services für Endbenutzer von GxP-Systemen bereit.</p>

GxP-Systemprinzip	Zusammenfassung der Anforderungen	Überlegungen
<b>Sicherung und Wiederherstellung</b>	Es sollten regelmäßige Sicherungen von GxP-Daten durchgeführt werden. Dazu gehört auch die Verifizierung der Datenintegrität und der Wiederherstellbarkeit.	<p>Kunde: Der Kunde ist beim Konfigurieren und Verwenden von AWS-Produkten dafür verantwortlich, angemessene Sicherheit, Sicherung und angemessenen Schutz der Daten aufrechtzuerhalten.</p> <p>AWS: AWS hat keinerlei Kontrolle über die kundenspezifische Konfiguration der Produkte und keine Einblicke in die Inhalte des Kunden (d. h., die Daten). Demzufolge nimmt AWS keine Sicherungen von Kundeninhalten im Namen von Kunden vor.</p>
<b>Vorfallreaktion</b>	GxP-Systemvorfälle sollten gemeldet, bewertet und dokumentiert werden.	<p>Kunde: Der Kunde ist dafür verantwortlich, Vorfallberichte von seinen Endbenutzern und Systemadministratoren zu erhalten, diese Berichte zu bewerten und zu dokumentieren. Wenn ein Vorfallbericht den Support von AWS erfordert, kann der Kunde über eine im Supportvertrag vereinbarte Methode einen Supportfall einreichen.</p> <p>AWS: AWS hat keinen Einblick in GxP-Systemvorfälle, jedoch werden Supportfälle, die an AWS übermittelt werden und die sich auf ein Problem mit AWS-Produkten beziehen, entsprechend der Supportvereinbarung des Kunden bewertet und untersucht. Kunden-Supportverläufe werden dokumentiert und für die Kunden online bereitgestellt.</p>
<b>Korrektur- und Präventivmaßnahmen</b>	Für GxP-Systeme sollten Maßnahmen zur Korrektur und Prävention von Systemabweichungen eingerichtet werden.	<p>Kunde: Der Kunde regelt die Erfassung und Nachverfolgung von GxP-Systemabweichungen. Er ist dafür verantwortlich, die erforderlichen Korrektur- und Präventivmaßnahmen umzusetzen.</p> <p>AWS: AWS hat keinen Einblick in die Systemvorgänge und -abweichungen und kann keine Korrektur- und Präventivmaßnahmen für das System umsetzen. AWS unterhält ein ständiges Verbesserungsprogramm für AWS-Produkte. Dieses Programm ist im Umfang der Qualitäts- und Sicherheitsbescheinigungen enthalten.</p>

Die Web-Service-Technologie erlaubt in Kombination mit modernen automatisierten Bereitstellungspraktiken die höhere Geschwindigkeit und Belastbarkeit von Systemen, die ständig weiterentwickelt werden, indem einzelne Systemkomponenten mit minimaler – und häufig gar keiner – Stillstandzeit des Systems oder Unterbrechung von Abhängigkeiten aktualisiert werden können. Solange die API-Schnittstellenspezifikation nicht geändert wird, kann der Kunde mit dem System interagieren und darauf vertrauen (durch Verifizierung), dass die genutzten Funktionen verfügbar sind. Kunden, die AWS-Produkte nutzen, profitieren von den Vorteilen von Web-Service-APIs. Allerdings müssen die Systeme dennoch auf Widerstandsfähigkeit gegen API-Ausfälle ausgelegt werden. API-basierte Systeme können auch in Änderungskontrollsysteme integriert werden, z. B. Remedy, ServiceNow, Sparta Systems und andere Änderungsmanagement-Nachverfolgungssysteme, wodurch eine vollständige Integration der Softwareentwicklungs- und Bereitstellungs-Pipeline in GxP-Abnahmeprotokolle gewährleistet ist.

Um diese betrieblichen Vorteile zu erlangen, sollten GxP-Kunden ihre Betriebsdokumente und -aufzeichnungen überprüfen und nötigenfalls aktualisieren, um sie mit der Nutzung von AWS-Produkten abzugleichen.

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- Änderungskontrollverfahren
- Konfigurationsverwaltungs-Verfahren
- Verfahren für Freigabe zur Produktion
- Überwachungsverfahren
- AWS CloudTrail- und Config-Protokolle
- Quellcode der Anwendung
- EC2 AMIs und CloudFormation-Vorlagen
- Kunden-Supportverläufe

### 3.3 Regulatorische Angelegenheiten

In GxP-regulierten Branchen verwenden Fachleute für regulatorische Angelegenheiten Daten aus GxP-Systemen zur Übermittlung von Einreichungen und Registrierungsdokumenten an Gesundheitsbehörden und Ethikausschüsse. Diese Fachleute entwickeln und unterhalten auch Verfahren zum Hosten von Prüfungen durch Regulierungsbehörden und halten sich auf dem neuesten Stand mit der sich ständig ändernden Gesetzgebung in den Regionen, in denen die Organisation ihre GxP-Produkte vertreiben will. Wenn ein GxP-Kunde AWS-Produkte in seinen GxP-Systemen verwendet, sollten seine IT-, Qualitäts- und Expertenteams für regulatorische Angelegenheiten besprechen, welche möglichen Auswirkungen sich auf den Umgang mit Behörden ergeben könnten. Dazu zählen

- Einreichungen bei Behörden und
- Prüfungen durch Gesundheitsbehörden sowie
- Anforderungen von Prüfungs- und Ethikausschüssen.

### 3.3.1 Einreichungen

Die Nutzung von GxP-Systemen für Zulassungsanträge ist nicht neu, und es gibt bereits cloudbasierte Software-Anwendungen zum Erstellen, Nachverfolgen und Absenden von Zulassungsanträgen. Tatsächlich verwendet die FDA AWS-Produkte zum Veröffentlichen von Daten aus Zulassungsanträgen über die Plattform openFDA.gov. Ein neuer Aspekt, der von GxP-Kunden berücksichtigt werden muss, ist die Frage, ob ihr GxP-System im Inhalt des Zulassungsantrags enthalten sein soll, und wenn ja, wie das Expertenteam des Kunden für regulatorische Angelegenheiten den Einsatz von AWS-Produkten einbringen soll.

Beispielsweise kann eine Software-Anwendung für ein medizinisches Gerät, z. B. ein Bildarchivierungs- und Kommunikationssystem (PACS), eine 510k-Einreichung für die FDA-Freigabe erfordern. Wenn das PACS für den Betrieb auf einem gewöhnlichen x86-Server ausgelegt ist, der mit dem Amazon EC2-Produkt von AWS kompatibel ist, sind in dem 510k des PACS die AWS-Produkte möglicherweise nicht im Einzelnen erwähnt. Die Formulierung lautet dann einfach: „Die Software-Anwendung ist ein PACS, das auf universellen Datenverarbeitungs-Servern betrieben wird.“ Die Entscheidung, AWS-Produkte in Zulassungsanträgen einzuschließen, obliegt der Verantwortung von GxP-Kunden. AWS rät diesen, bei Fragen in Verbindung mit Zulassungen einen qualifizierten Rechtsbeistand zurate zu ziehen.

### 3.3.2 Prüfungen

Die Gesundheitsbehörden können Life-Sciences-Organisationen und deren GxP-Systeme jederzeit überprüfen. Obwohl COTS-IT-Produkte schon seit längerer Zeit in GxP-Systemen verwendet werden, die durch Behörden überprüft wurden, ist die Nutzung von COTS-Cloud-Produktanbietern wie AWS in GxP-Systemen relativ neu, und die behördlichen Prüfer sind möglicherweise mit AWS-Produkten oder deren Verwendung nicht vertraut. Um ein erfolgreiches Prüfergebnis bei GxP-Systemen sicherzustellen, die AWS-Produkte nutzen, empfiehlt AWS GxP-Kunden, einen Prüf-Bereitschaftsplan zu erstellen und aufrechtzuhalten, der mehrere Elemente enthält:

- Benennung der wichtigsten Personen in der Organisation des Kunden, die mit der Konfiguration und Nutzung von AWS-Produkten im GxP-System vertraut sind,
- Verfahren, um sicherzustellen, dass diese wichtigen Personen im Fall einer FDA-Prüfung benachrichtigt werden und verfügbar sind sowie
- eine Präsentation mit einer allgemeinen Übersicht über jedes einzelne GxP-System, um dem Prüfer der FDA oder Gesundheitsbehörde schnell und präzise die wichtigsten Systemelemente aufzuzeigen. Die Kunden sollten die folgenden Elemente in ihre Präsentationsmaterialien aufnehmen:
  - Systemidentifikation einschließlich Systembezeichnung, Version (falls zutreffend) und Systemklassifizierung
  - Systembeschreibung einschließlich einer allgemeinen Übersicht über die wichtigsten GxP-Aktivitäten und/oder Tätigkeitsfunktionen, die vom System abhängig sind; Schnittstellen zu anderen Systemen sollten ebenfalls benannt werden
  - Netzwerk- oder Architekturdiagramm einschließlich aller hiermit verbundenen Verantwortlichkeiten
  - Systembetrieb einschließlich physischer Standorte, an denen auf das System zugegriffen werden kann, Anzahl der Endbenutzer, Schnittstellen und Produkte
  - Liste von Anwendungs-SOPs einschließlich aller technischen, Geschäftsbereichs- oder Unternehmensverfahren
  - Zusammenfassung der Verantwortlichkeiten einschließlich des/der Namen(s) der Endbenutzer-Geschäftseinheit(en), technischer und administrativer Verantwortlichkeit, Sicherheitsoperationen usw.

Im Fall einer systembezogenen Untersuchung, die Support von AWS bei der Produktfehlersuche erfordert, bestimmt die vom Kunden gewählte AWS-Supportstufe die Methode zur Übermittlung von Support-Anfragen und die zu erwartende Reaktionszeit von AWS.

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- Prüf-Bereitschaftsplan
- Präsentation mit Übersicht des GxP-Systems
- System-Dokumentationsindex

### 3.3.3 Datenschutzkontrollen für die personenbezogenen Daten von Forschungsteilnehmern

GxP-Systeme, die in der klinischen Forschung verwendet werden, können auch Datenschutzkontrollen erfordern, um die Vertraulichkeit der Daten von Personen zu gewährleisten, deren personenbezogene Informationen (Personally Identifiable Information, PII) und geschützte Gesundheitsdaten (Protected Health Information, PHI) vom System gespeichert, verarbeitet oder übertragen werden. Beispiele hierfür sind:

- Forschungs-Rekrutierungstools,
- elektronische Datenerfassungssysteme (EC-Systeme),
- Datenspeicherung und -archivierung,
- diagnostische medizinische Geräteanwendungen und
- mobile medizinische Geräteanwendungen.

Sponsoren und Forscher, die Forschungsstudien am Menschen mithilfe von GxP-Systemen durchführen, die AWS-Produkte enthalten, können von institutionellen Prüfungskommissionen (Institutional Review Boards, IRB), unabhängigen Ethikausschüssen (Independent Ethics Committees, (IEC) und/oder Datenzugriffsausschüssen (Data Access Committees, DAC) aufgefordert werden, Informationen darüber zu geben, wie das System personenbezogene Informationen von Studienteilnehmern sichert, einschließlich aller durchgeführten Systemsicherheitsprüfungen und Sicherheitsfunktionskontrollen, z. B. eine Beschreibung der Verfahren zur Aufhebung des Systemzugriffs, wenn dieser nicht länger erforderlich ist. Kunden, die AWS-Produkte in GxP-Systemen nutzen, die PII enthalten, sollten sich mit den Datenlokalitätsanforderungen vertraut machen und nötigenfalls die Sicherheits- und Datenlokalitätskontrollen beschreiben, die in die AWS-Produkte implementiert sind, mit denen das System betrieben wird. Weitere Informationen über Datenlokalitätskontrollen in AWS-Produkten sind online verfügbar unter <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>.

Die Kunden sollten die folgenden Dokumente aktualisieren, um die Nutzung von AWS-Produkten in GxP-Systemen zu optimieren:

- Richtlinie zum Schutz personenbezogener Daten
- Datenlokalitäts-Kontrollplan
- System-Sicherheitsplan für GxP-Systeme

## 4 SCHLUSSFOLGERUNG

Obwohl die Bereitstellung von AWS-Produkten über das Internet und nicht physisch erfolgt, verbleibt die Zuständigkeit und Verantwortlichkeit für die Nutzung der Produkte bei den GxP-Kunden, einschließlich der Anwendungen und virtualisierten Infrastruktur, die sie mithilfe von AWS-Produkten entwickeln, validieren und betreiben. Mit den Empfehlungen in diesem Whitepaper können GxP-Unternehmen ihre Qualitätssysteme, SDLC-Kontrollen und Pläne für Zulassungsangelegenheiten bewerten, um die effektive Kontrolle über GxP-Systeme aufzuzeigen, in die AWS-Produkte als Bestandteil integriert sind.

## 5 AM DOKUMENT VORGENOMMENE ÄNDERUNGEN

Die unten stehende Tabelle zeigt den kompletten Änderungsverlauf für dieses Whitepaper.

<b>Datum</b>	<b>Beschreibung</b>
<b>Januar 2016</b>	<b>Erstversion</b>

## 6 ANHÄNGE

### 6.1 Datenschutz-Ressourcen

Bei AWS hat der Datenschutz stets oberste Priorität. Obwohl die Kontrolle und der Besitz der Daten bei der Nutzung von AWS-Produkten bei den Kunden verbleiben, bemüht sich AWS intensiv, zusätzliche Datenschutzfunktionen und Transparenz für die Kunden bereitzustellen. In diesem Anhang sind einige der wichtigsten Datenschutzressourcen aufgelistet, die AWS für die Kunden bereitstellt.

- Häufig gestellte Fragen zum Datenschutz von AWS  
<https://aws.amazon.com/compliance/data-privacy-faq/>
- Halbjährlicher Informations-Anfragebericht des Unternehmens Amazon  
[http://do.awsstatic.com/certifications/Information\\_Request\\_Report.pdf](http://do.awsstatic.com/certifications/Information_Request_Report.pdf)
- AWS-Liste von Dritten mit Zugriff  
<http://aws.amazon.com/compliance/third-party-access/>
- US-EU SAFE HARBOR  
<https://safeharbor.export.gov/companyinfo.aspx?id=27379>
- EU-Richtlinie 95/46/EC – Häufig gestellte Fragen und Modellklauseln  
<https://aws.amazon.com/compliance/eu-data-protection/>  
<http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html>
- US-Datenbank mit Genotypen und Phänotypen  
[https://do.awsstatic.com/whitepapers/compliance/AWS\\_dBGaP\\_Genomics\\_on\\_AWS\\_Best\\_Practices.pdf](https://do.awsstatic.com/whitepapers/compliance/AWS_dBGaP_Genomics_on_AWS_Best_Practices.pdf)
- US HIPAA – Geschäftspartner – Häufig gestellte Fragen  
<https://aws.amazon.com/compliance/hipaa-compliance/>

## 6.2 21 CFR Part 11 kommentiert

Dieser Anhang erläutert einige Möglichkeiten, wie Kunden AWS-Produkte so nutzen können, dass die Anforderungen für elektronische Aufzeichnungen und elektronische Signaturen gemäß den Bestimmungen von 21 CFR Part 11 erfüllt sind.

- **Zugriffskontrollen:** Der Zugriff auf GxP-Systeme und -Daten kann von den Kunden auf autorisierte Personen beschränkt werden. Die Kunden können AWS-Produkte nutzen, z. B. Amazon Identity and Access Management (IAM) und AWS Directory Service, um Zugriffskontrollen zu implementieren. AWS-Kunden können auch ihre Konto-Zugriffskontrollen so konfigurieren, dass sie mit bereits bestehenden, vor Ort eingerichteten Verzeichnissen wie Microsoft Active Directory zusammenarbeiten, so dass sich eine nahtlose Zugriffskontrollumgebung für hybride Cloud-Bereitstellungen ergibt.
- **GxP-Systemvalidierung:** Anwendungen können in AWS bereitgestellt und validiert werden. Die Kunden können ihre GxP-Systeme nach den Richtlinien und Verfahren ihrer Organisation validieren.
- **Abrufbarkeit von Daten:** Richtige und vollständige Kopien von Aufzeichnungen können erstellt und von AWS-Kunden jederzeit während des Aufbewahrungszeitraums über ihr AWS-Konto abgerufen werden. Weil AWS-Kunden vollständigen administrativen Zugriff auf ihr AWS-Konto, die Systeme und Daten haben, können sie ihre Daten oder Prüfpfade jederzeit unabhängig abrufen, vorausgesetzt, dass der Kunde die AWS-Prüfpfad-Produkte und -Funktionen aktiviert hat.
- **Prüfpfade:** Sichere, computergenerierte und mit Zeitstempel versehene Prüfpfade können nach vom Kunden definierten Richtlinien generiert, überwacht, heruntergeladen und gespeichert werden. AWS-Produkte wie AWS CloudTrail und Amazon CloudWatch erlauben es den Kunden, Protokollierungssysteme zu entwickeln und zu betreiben, die die höchsten Daten- und Systemprüfungsstufen erfüllen, von der Ebene einzelner Dateiobjekte bis zur Anwendungsebene.
- **Workflow-Durchsetzung:** Betriebssystem-Prüfungen für GxP-Workflow-Aktivitäten werden vollständig von den AWS-Kunden kontrolliert, einschließlich der SDLC-Prozesse, die sie für das GxP-System unterhalten.
- **Benutzer-Autorisierung:** Autorisierungsprüfungen, die sicherstellen sollen, dass der jeweilige Benutzer berechtigt ist, das System zu benutzen oder Daten zu verändern, können von AWS-Kunden mit Rollen und Berechtigungsgruppen auf Infrastruktur-Ebene innerhalb des AWS-Kontos oder der Anwendungen implementiert werden. Produkte wie Amazon IAM ermöglichen es den Kunden, die Rollen, Sicherheitsebenen und Transaktionsrichtlinien zu definieren, die sie für Infrastruktur-Benutzerkonten sowie für Servicekonten von Maschine zu Maschine benötigen.
- **Eingangs-/Ausgangsverifizierung:** Eingangsprüfungen und Nachweisbarkeitskontrollen hängen in hohem Maß von den Personen, Prozessen und Technologien ab, die die GxP-Daten erstellen und aktualisieren. Wenn GxP-Daten manuell in eine Web- oder Mobilanwendung eingegeben werden, können AWS-Kunden eine Kombination aus manuellen Prozessen nutzen, um Benutzer zu schulen und zu verifizieren, bevor ihnen der Zugang zu der Anwendung gewährt wird. Wenn der Zugriff gewährt wurde, können die Kontrollen auf Anwendungsebene die erforderlichen Eingangsprüfungen automatisch aktivieren. Die AWS-Produkte innerhalb des Kundenkontos können zum Überwachen und Kontrollieren der Konnektivität vernetzter Ressourcen verwendet werden, z. B. Workstations oder Mobilgeräte. Wenn GxP-Daten automatisch von örtlichen Instrumenten, Gerätesensoren oder Datenverarbeitungsprozessen einer Anwendung generiert werden, können das Einreihen in die Warteschlange und der Transport der Daten von der lokalen Umgebung des Kunden zu dessen AWS-Konto mit einer Reihe von AWS-Produkten aktiviert und kontrolliert werden, beispielsweise Amazon Simple Queue Service (SQS) und Amazon Kinesis, sowie mit den Identity and Access Management-Tools, mit denen Zugriffskontrollen auf Benutzer- und Service-Ebene aktiviert werden.



- **Personalschulung:** AWS-Kunden entwickeln, unterhalten und nutzen die GxP-Daten und -Systeme in ihrem AWS-Konto. Das heißt, sie können ihre bestehenden Richtlinien und Verfahren befolgen, um zu ermitteln, ob ihre Mitarbeiter die Ausbildung, Schulung und Erfahrung haben, um die ihnen zugewiesenen GxP-Aufgaben durchzuführen. AWS bietet umfassende technische Dokumentationen und Kundenschulungsprogramme an, um den IT-Engineering-Mitarbeitern des Kunden dabei zu helfen, ihre AWS-Lernziele zu erreichen. Das umfangreiche AWS-Partner-Ökosystem beinhaltet Systemintegratoren von Drittanbietern sowie Beratungspartner mit Fachwissen in den Bereichen Gesundheitswesen und Life Sciences.
- **Systemdokumentation:** Eine angemessene Kontrolle der Systemdokumentation kann mit den bestehenden kundenseitigen Dokumentenkontrollverfahren und -systemen erreicht werden. Die technische Dokumentation von AWS sowie alle versionsspezifischen Informationen, die der Kunde benötigt, können über die entsprechende URL abgerufen werden. Weil darüber hinaus die virtuelle Infrastruktur, die die einzelnen Kunden in AWS einrichten, naturgemäß eine softwaredefinierte Infrastruktur ist, können die Kunden den kompletten Code-Satz und die Vorlagen, die sie zum Definieren der AWS-Ressourcen in ihrem Konto verwenden (siehe „Qualifizierte Infrastruktur“), über die Version steuern und archivieren.
- **Sicherheitskontrollen:** Zusätzliche Maßnahmen, beispielsweise die Verschlüsselung von Daten im Ruhezustand und im Transit, können von den Kunden mit ihren bestehenden clientseitigen Verschlüsselungslösungen oder mit dem umfangreichen Sortiment an Sicherheitsprodukten von AWS umgesetzt werden, z. B. Amazon Key Management Service (KMS), sowie mit serverseitiger Verschlüsselung, transparenter Datenverschlüsselung (TDS) und Secure Socket Layer- (SSL-) Funktionen in Produkten wie Amazon Simple Storage Service (S3), Amazon Relational Database Service (RDS) und Amazon Elastic Load Balancer (ELB). Amazon Virtual Private Cloud (VPC) ist ein Produkt, mit dem Kunden ihre virtuelle Netzwerkumgebung kontrollieren und verschlüsselte Hardware Virtual Private Network- (VPN-) Verbindungen zwischen ihrem lokalen Rechenzentrum und ihrer Amazon VPC erstellen können, um so die Cloud als Erweiterung ihres bestehenden Netzwerks nutzen zu können.
- **Elektronische Signaturen:** Anforderungen für elektronische Signaturverzeichnisse, Signatur-/Aufzeichnungsverknüpfungen sowie elektronische Signaturkomponenten und -kontrollen werden normalerweise im Rahmen der validierten Anwendungen erfüllt, die die Kunden zum Erzeugen und Unterhalten ihrer GxP-Daten verwenden. Die Kunden sollten die Eignung ihrer bestehenden elektronischen Signaturanwendungen für das virtuelle Netzwerk in ihrem AWS-Konto überprüfen. Sie können die elektronischen Signaturanforderungen auch als Bestandteil der angepassten, in der Cloud verfügbaren Anwendungen erfüllen, die sie selbst entwickeln. Wenn AWS-Produkte zur Erfüllung von Anforderungen wie Passwortkontrollen verwendet werden, können gebrauchsfertige Funktionen wie die Amazon IAM-Passwortrichtlinien es den Kunden ermöglichen, nach ihren jeweiligen Bedürfnissen ihre eigenen Richtlinien für die Passwort-Komplexität und -Geltungsdauer zu entwickeln.
- **Datenaufbewahrung:** Die Verfahren und Richtlinien für den Lebenszyklus und den Aufbewahrungszeitraum der GxP-Daten hängen in hohem Maß von der Organisation und den jeweils geltenden Anforderungen des einzelnen Kunden ab. Beim Entwerfen und Entwickeln von GxP-Datenmanagement-Lösungen in ihrem AWS-Konto sollten die Kunden darauf achten, ihre Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit festzulegen, einschließlich aller Aufbewahrungsrichtlinien für Rohdaten, abgeleitete Daten und Metadaten.

### 6.3 Gemeinsame Verantwortlichkeiten in AWS-Vereinbarungen

Diese Tabelle gibt einen Überblick über die in AWS-Standardverträgen aufgeführten Verantwortlichkeiten und ist nicht verbindlich. Die in diesem Abschnitt dargelegten Verantwortlichkeiten gelten nur für die einzelnen AWS-Produkte und enthalten nicht die zwischen AWS-Kunden und ihren Endbenutzern festgelegten SLA-Verantwortlichkeiten.

Thema	Verantwortlichkeiten	Kunde	AWS
Kontakte	Eine gültige, mit dem AWS-Konto verknüpfte E-Mail-Adresse aufrechterhalten (Kundenvertrag 1.2)	x	
Änderungen	Kunden über wesentliche Änderungen oder Einstellungen von AWS-Produkten benachrichtigen (Kundenvertrag 2.1)		x
Änderungen	Frühere Versionen von AWS-Produkt-APIs 12 Monate lang unterstützen (Kundenvertrag 2.2)		x
Änderungen	Nach Bedarf Sicherheitsaktualisierungen durchführen, um Vertraulichkeit, Integrität und Verfügbarkeit von AWS-Produkten sicherzustellen <a href="https://aws.amazon.com/security/security-bulletins/">https://aws.amazon.com/security/security-bulletins/</a>		x
Inhalt	Entwicklung, Inhalt, Betrieb, Instandhaltung und Nutzung des Inhalts (d. h., GxP-Aufzeichnungen und -Anwendungen) (Kundenvertrag 4.1)	X	
Inhalt	Sicherheit, Schutz und Sicherung des Inhalts (Kundenvertrag 4.2)	x	
Support	Support für Endbenutzer des GxP-Systems bereitstellen (Kundenvertrag 4.2)	x	
Support	Basic Support für Kunden <a href="https://aws.amazon.com/premiumsupport/">(https://aws.amazon.com/premiumsupport/)</a>		x
Datenschutz	Kontrolle der geographischen Regionen, in denen die Daten gespeichert werden	x	